IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

Appendix 1 - Comments Received in Response to Rules Notice 18-0070 – Rules Notice – Request for Comments – Dealer Member Rules – Amendments Respecting Mandatory Reporting of Cybersecurity Incidents

On April 5, 2018, we issued Notice 18-0070 requesting comments on amendments (**Amendments**) to the Dealer Member Rules (**DMRs**) and the IIROC Dealer Member Plain Language Rule Book (the **PLR Rule Book**) relating to mandatory reporting of cybersecurity incidents by Dealer Members (**Dealers**) to IIROC. IIROC received eight comments letters from the following commenters:

Assante Wealth Management Ltd.
Desjardins Securities Inc.
Investment Industry Association of Canada
IGM Financial Inc.
Fidelity Clearing Canada ILC
Manulife Securities
MD Management Limited
SIFMA

Copies of these comments are publicly available on IIROC's website. The following table summarizes these comments and our responses:

	Summary of Comment	IIROC Response
General Comments		
1.	Overall, most commenters are supportive of IIROC's approach and are committed to making cybersecurity risk management a priority. Commenters recognize that reporting cybersecurity incidents is an essential tool for mitigating cyber threats that will benefit Dealers and the public.	Thank you for your comments.
2.	The current reporting structure required through the Privacy Commission under the *Privacy Information Protection and Electronic Documents Act* (**PIPEDA**), as well as regulatory bodies such as the Office of the Superintendent of Financial Institutions (**OSFI**) could be leveraged to provide IIROC with information, rather than creating a new, parallel system of reporting.	We have endeavoured to align the Amendments with the reporting requirements under PIPEDA and OSFI as far as reasonably possible. However, we note: (i) not all Dealers are subject to OSFI oversight, and

	Summary of Comment	IIROC Response
	Under OSFI *Major Cyber Security Incident Reporting*, which several Dealers are subject to, Dealers are required to report certain incidents. In determining whether to report, OSFI requires Dealers to consider: • impact to key/critical Information Systems/Data • severe operational impact to internal users • significant and serious levels of system/service disruptions • severe and extended disruptions to critical business systems/operations • number of external customers impacted is large or growing • negative reputational impact is imminent • incident reported to public authorities. Given the provision seems to be addressing the same type of harm (to individuals), and that the Amendments requires reporting whether other "applicable laws" require notice to any "government body, securities regulatory authority or other self-regulatory organization", it would be useful to harmonize or defer to PIPEDA or OSFI standards as applicable. By adopting PIPEDA reporting requirements, IIROC would be aligned with current guidance from the Privacy Commissioner of Canada and the mandatory breach reporting regulations in the European Union. IIROC should also consider accepting reports filed under PIPEDA or OSFI requirements on the same timelines. Dealers should not experience additional regulatory burdens at the time when resources should be committed to responding to cybersecurity incidents and reporting to other regulators.	(ii) while all Dealers are subject to the PIPEDA reporting requirements (which came into force in November 2018), the objectives of PIPEDA are slightly narrower than the Amendments. PIPEDA focuses specifically on the protection of *personal information* (any factual or subjective information about an identifiable individual) and significant harm *to the individual*. The Amendments capture any report a Dealer may submit under section 10.1 of PIPEDA. However, the Amendments also require reporting of cybersecurity incidents beyond breaches involving an individual's personal information and the significant harm to an individual. It includes incidents related to information systems that results in, or has a reasonable likelihood of resulting in, substantial harm to a non-individual (like an Institutional Customer). In light of IIROC's mission to protect investors, strengthen market integrity and support healthy Canadian capital markets, the objectives of the Amendments are slightly broader than those under PIPEDA. Merely relying on reports that Dealers submit under PIPEDA or OSFI's Cyber Security Incident Reporting requirements would be insufficient as it would not capture all relevant Dealers nor all relevant cybersecurity incidents.

	Summary of Comment	IIROC Response
3.	PIPEDA requires the organizations to notify "any other organization that may be able to mitigate harm to affected individuals", which ought to obligate Dealers to report a security breach to IIROC and/or other securities regulators as appropriate. The Amendments duplicate the reporting requirements. If IIROC requires Dealers to comply with PIPEDA, Dealers will also satisfy reporting obligations to IIROC.	The Amendments are consistent with but do not entirely duplicate the notification obligations under section 10.2(1) of PIPEDA. This section requires concurrent notification to an individual affected by a breach as well as to any organization that may be able to reduce the risk of harm that could result from the breach to the affected individuals. The Amendments require reporting that is more specific than the notification required under section 10.2(1) of PIPEDA in two important ways: (i) the Amendments specify the specific timing and content of the report to be provided to IIROC, whereas PIPEDA merely refers to "notification", (ii) the Amendments ensure prompt cybersecurity incident reporting to assist IIROC in more than just immediate support to the affected Dealer. The reporting also helps IIROC alert other Dealers of threats, where necessary, evaluate trends and promote confidence in the Dealer and integrity in the market. The notification trigger under section 10.2(1) of PIPEDA is limited to IIROC's ability to "mitigate harm to affected individuals". As IIROC's objectives in mandating cybersecurity incident reporting extends beyond just mitigation of harm to affected individuals, the notification

	Summary of Comment	IIROC Response
		under PIPEDA does not fully achieve IIROC's desired policy objectives.
4.	IIROC should carry out additional consultations with the Dealers about cybersecurity practices for their comments on the potential significant and or unforeseen costs that may be associated with the Amendments.	The Amendments are informed by the ongoing cybersecurity work IIROC has conducted with Dealers over the past three years. Additionally, following publication IIROC discussed the Amendments with a number of IIROC's Advisory Committees. In addition, IIROC utilizes the public comment period to obtain feedback in respect of the Amendments, including any significant and unforeseen costs that might be associated with the Amendments.
Definition of "cybersecurity incident"		
5.	The definition of "cybersecurity incident" adds several elements that are not clearly defined. This potentially materially expands the scope of the reporting requirement, without demonstrable benefits that would justify the additional reporting burden.	The Amendments were drafted to be consistent with IIROC's principles-based approach to rule-making. The definition of "cybersecurity incident" was intentionally drafted in a flexible manner to accommodate the evolving nature and variety of cybersecurity threats. Additionally, the Amendments allow for different Dealer business models. Cybersecurity incidents may have a different impact on a Dealer's operations depending on the nature of the Dealer's business model and the type of cybersecurity incident.
6.	IIROC should consider adopting the definition of "cybersecurity incident" under PIPEDA. This definition includes the concept of "breach of security safeguards" and "a real risk of significant harm" test.	As noted in response to comment #2, the objectives of PIPEDA are narrower than the Amendments. Adopting the definition of "cybersecurity incident" to mirror PIPEDA

	Summary of Comment	IIROC Response
		may result in excluding from reporting certain incidents unrelated to breaches involving personal information (as defined under PIPEDA) that nonetheless relate to broader issues of investor protection and maintaining healthy and efficient capital markets. We drafted the definition of "cybersecurity incident" under the Amendments to include those incidents which could affect a Dealer's ability to meet its obligations to its clients and capital market counterparties. The reporting threshold established by the Amendments include the concept of "reasonable likelihood of significant harm".
7.	PIPEDA regulations contains a reporting requirement where there is a "real risk of significant harm", where "significant harm" is defined to include bodily harm, humiliation, damage to reputation or relationships, loss or employment, business or professional opportunities, financial loss, identify theft, negative effects on the credit record and damage to or loss of property." The Amendments requires reporting where there is a "reasonable likelihood" of an incident resulting in "substantial harm or inconvenience to any person". How does "real risk" differ from "reasonable likelihood" and "significant harm" differ from "substantial harm"?	"Real risk" and "reasonable likelihood" are similar concepts, but must be understood in their context. According to guidance released by the Office of the Privacy Commissioner (**OPC**), in determining whether a breach of security safeguards create a real risk of significant harm, organizations may consider the probability that the personal information has been, is being, or will be, misused. Similarly, in determining where there is a "reasonable likelihood" of an incident resulting in "substantial harm" to any *person*, we expect Dealers to consider the probability of substantial harm to any *person* (which may include harm to a non-individual client) relating to more than just misuse of personal information (although that is included).

	Summary of Comment	IIROC Response
		"Substantial harm" includes the concepts listed in the definition of "significant harm" under section 10.1(7) of PIPEDA, but may encompass other types of harm to non-individuals. In contrast, PIPEDA's non-exhaustive list focuses on harm to an individual person and would likely be interpreted to exclude harm to non-individuals like corporations.
8.	The federal and provincial privacy laws allow some discretion for organizations to consider whether incidents create a "real risk of significant harm" to an individual. IIROC should consider a similar level of discretion when assessing cybersecurity incidents. This would also be consistent with the approach taken by OSFI.	Yes, we expect Dealers to exercise a level of discretion in determining whether an incident has a reasonable likelihood of resulting in any of the outcomes listed in Rule 3100, I.B. 1.1, section (1)(i) to (iv) [PLR Rule 3703(1)(i)- (iv)].[1]
9.	What is meant by "inconvenience"? If the computer of a Dealer's employee needs to be wiped clean as a result of the Dealer's security protocol, does this constitute "inconvenience"? What if that same computer was owned by an advisor who is an agent of the Dealer and not an employee and the computer contained information contained data pertaining to an outside business activity? Does the inconvenience need to impact the investor before it is meets the reporting threshold?	We intended the word "inconvenience" to be qualified by the word "substantial". Nevertheless, we have considered these comments and how "substantial inconvenience" could be interpreted to unreasonably expand the scope of the Amendments. Accordingly, we have removed "inconvenience" from the Amendments.

[1] When referencing specific subsections of the Amendments, we will be citing the DMRs sections with corresponding PLR Rule Book sections in square brackets.

	Summary of Comment	IIROC Response
10.	IIROC should consider removing the reference to "inconvenience" as it sets the threshold too low for an effective reporting regime.	As noted above, we have considered this comment and removed "inconvenience" from the Amendments.
11.	The reference to "any act to gain unauthorized access" is overly broad and would require Dealers to report any *attempt* to access data that is not authorized. The incidents that are actually important to report should be any *successful* unauthorized access. Dealers have sophisticated security systems and protocols that routinely block attempts by malware and other attempts to access their system. One commenter noted that their internal systems produce roughly 2,300 alerts per week that could potentially be characterized as cybersecurity incidents by the Amendments, of which 103 are "flagged" or further investigation and from which only 2-3 issues per month on average are reported internally. The Amendments may give rise to daily reporting of unsuccessful attempts. This may unduly tax IIROC resources.	While the definition of "cybersecurity incident" includes reference to "any act to gain unauthorized access", Dealers are only expected to report to IIROC those that resulted in, or had a reasonable likelihood of resulting in: (i) substantial harm or inconvenience to any person, (ii) a material impact on any part of the normal operations of the Dealer, (iii) invoking the Dealer's business continuity plan or disaster recovery plan, or (iv) the Dealer being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization. We have avoided defining cybersecurity incident as either successful or unsuccessful. Rather, we have made reporting conditional on the foregoing listed outcomes taking place or the Dealer determining there is a reasonable likelihood of the foregoing taking place.
12.	Requiring reporting where there is "material impact on any part of the normal operations of the *Dealer Member*" creates uncertainty and inconsistency with the requirements under PIPEDA, and appears more stringent than the OSFI requirements. Where an incident creates a material impact on the normal operations of a Dealer, but does not put any client data at risk or affect operations that would materially affect service to clients, it is unclear why this would require reporting. This may create an additional burden to firms without	IIROC requires reporting in instances where a cybersecurity incident affects the normal operations of a Dealer, but does not put client data at risk, because IIROC's mission includes strengthening market integrity and supporting healthy Canadian capital markets. To achieve this objective, IIROC monitors Dealers' financial condition and business activities within prescribed capital

	Summary of Comment	IIROC Response
	commensurate benefits to the industry. The reference to "normal operations" should be qualified to ensure these operations are material to client data security.	and operational rules. As noted in response to comment #6, we drafted the definition of "cybersecurity incident" under the Amendments to include those incidents which could affect a Dealer's ability to meet its obligations to its clients and capital market counterparties, and by implication, threaten market integrity and a healthy Canadian capital market. Furthermore, we expect that any incident that creates a material impact on the normal operations of a Dealer would likely materially affect service to the clients. Qualifying the definition of cybersecurity incident to reference only operations that are material to client data security would inappropriately limit the scope of the Amendments.
13.	Would an incident that slows down the firm's website or internal systems be the type of matter that would be subject to the Amendments?	An incident that slows down the firm's website or internal systems would be subject to reporting under the Amendments only if the incident arose from an act to gain unauthorized access to the information system or information story on the information system that resulted in, or had a reasonable likelihood of resulting in: (i) substantial harm or inconvenience to any person, (ii) a material impact on any part of the normal operations of the Dealer, (iii) invoking the Dealer's business continuity plan or disaster recovery plan, or

	Summary of Comment	IIROC Response
		(iv) the Dealer being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization. Accordingly, if the incident slowed down the firm's internal system in a manner that had a material impact on any part of the Dealer's normal operations, then we would expect the Dealer to report under the Amendments.
14.	The categorization of impact as "material" will likely vary as between very large and small firms, and this should be taken into account. Dealers should have discretion in determining what is material for their particular operation.	We agree that "material" will vary between Dealers of different sizes and recognize that Dealers will need to exercise judgment in determining what constitutes a "material impact" on their normal operations.
15.	IIROC should clearly articulate the circumstances under which a report should be filed with IIROC, so firms are not over or under-reporting cybersecurity incidents. The definitions of "substantial harm", "inconvenience" and "material impact" should be illustrated with examples and guidance, developed in discussion with Dealers.	While IIROC seeks to assist Dealers to understand the new reporting obligation, we must also recognize the complex and rapidly evolving nature of cybersecurity threats. We want to avoid issuing guidance that may quickly become obsolete. However, we will consider developing guidance following implementation of the Amendments.
16.	The definition of "cybersecurity incident" contained in the Amendments should distinguish between a cybersecurity incident and a privacy incident. Privacy incidents often arise from human errors whereas cybersecurity incidents usually result from an attempt to misuse Dealer data or client assets by a third party. The measures taken to correct the incidents differ.	Rather than view cybersecurity incidents and privacy incidents as separate and distinct concepts, we see potential overlap between the two. A cyber-related incident may result in the inappropriate disclosure of personal information. Accordingly, such incident would

	Summary of Comment	IIROC Response
		potentially be considered both a privacy incident and cybersecurity incident.
17.	The Amendments definition of "cybersecurity incident" includes "a material impact on any part of the normal operations of the Dealer Member." Section 500.17(a)(2) of the New York State Department of Financial Services Cybersecurity Regulation[2] provides "Cybersecurity Events that have a reasonable likelihood of materially harming any *material* part of the normal operation(s) of the Covered Entity". As a result of the work "material" being absent from the Amendments, an unintentional consequence is that an incident that has a "material impact" of a negligible or insignificant part of a Dealer's normal operation is now reportable. For example, a Dealer may have a non-material shopping website selling promotional merchandise with its corporate logos. Even though this website is only a very small part of the business of the Dealer's normal operation and has no meaningful connection to its investment and trading operations regulated by IIROC, one may conclude that a disruption of the website would be reportable to IIROC under the Amendments. IIROC should consider adding the work "material" so the definition reads "a material impact on any *material* part of the normal operations of the Dealer Member" (emphasis added).	Introducing a further materiality threshold in the proposed manner may unduly narrow the scope of the reporting obligation. IIROC rules contain requirements for Dealers and their registered employees relating to, among others, business conduct, financial operations and trading practices. Using the term "normal operations" reflects the range of IIROC's regulatory oversight of its Dealers. Under the proposed hypothetical, a Dealer would have to report a "disruption of the website" only if it resulted in (or had a reasonable likelihood of resulting in) a material impact on the Dealer's normal operation. The materiality of the incident on the normal operations of the Dealer triggers a report under the Amendment.
18.	The invocation of a business continuity or disaster recovery plan is a substantially different threshold than other definitions of a "cybersecurity incident". Since DMR 3100(i)(B)(1.1)(1)(iii)/PLR 3703(1)(iii) does not indicate a "materiality" threshold, IIROC should strike this from the definition.	The materiality concept is implied in DMR 3100(i)(B)(1.1)(1)(iii)/PLR 3703(1)(iii). Where a Dealer invokes its business continuity plan or its disaster recovery plan, we expect that this would be in response to a material event. Under DMR 17.16 (PLR 4712), a

[2] See "23 NYCRR 500. New York Department of Financial Services Proposed Cybersecurity Requirements for Financial Services Companies." (DFS Proposal) https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

	Summary of Comment	IIROC Response
		Dealer's business continuity plan identifies the procedures it will take to deal with a significant business disruption.
Timing of Reporting		
19.	The timing for reports under the Amendments differs from the timing under PIPEDA, OSFI and provincial privacy regulations. PIPEA requires one report filed "as soon as feasible after the organization determines that the breach has occurred" with the ability to file updates as information becomes available. This reporting structure permits an organization to conclude a detailed investigation before having to report a breach on incomplete analysis of facts. OSFI requires timely notification of major cybersecurity incidents. Alberta's privacy regulations requires reporting "without unreasonable delay". The 3-day and 30-day reporting deadlines in the Requirements may not allow for meaningful assessment of a security incident prior to reporting to IIROC. In one commenter's experience, a cybersecurity attack or incident can require considerable effort to properly identify, assess and then remediate, especially if the scope of the threat or incident is significant. Early reporting is important, but mandating a report within three calendar days of discovery may not offer any material insights with respect to assessment or remediation. Additionally, 30 days may be insufficient for a Dealer to complete an incident investigation. The timelines contained in the Amendments should provide maximum flexibility to fulfil their statutory obligations in a manner compatible with their particular circumstances.	We intended the three-day report to reflect only a preliminary assessment of the cybersecurity incident. The three-day report is not usually/normally intended to reflect material insights respecting assessment or remediation. We recognize that three calendar days following discovery of the cybersecurity incident, a Dealer may have an incomplete analysis or analysis that will later be updated upon full investigation. However, timely reporting of the core features of a cybersecurity incident is central to accomplishing the objectives of the Amendments, especially where the cybersecurity incident could potentially affect other Dealers or threaten the capital market system more generally. Furthermore, the Amendments expressly provide for flexibility in submitting an incident investigation report after 30 days, with agreement from IIROC.
20.	The reporting process should mirror the requirements of existing regulations, such as reporting within 5 business days in accordance with the OSFI guidelines, following which the Dealer negotiates a time for more detailed reporting with IIROC or abides by a 90 day timeframe to provide IIROC with a final report detailing its steps to identify, contain, respond and remediate the cybersecurity incident. These proposed timeframes are	We believe prescriptive timeframes are necessary to eliminate ambiguity in reporting timeframes and ensure timely reporting of cybersecurity incidents. The timeframes reflected in the Amendments reflect the

	Summary of Comment	IIROC Response
	consistent with other reporting requirements, such as responding to requests for personal information under applicable privacy laws, and when responding to client complains under applicable Mutual Fund Dealers Association and IIROC requirements. The timeframes for reporting should be less prescriptive.	specific nature of cybersecurity risks that demand timely response and information sharing. The Amendments also expressly contemplate Dealers requesting additional time for submitting the 30-day report.
21.	The three-day IIROC requirement from discovery of the incident may in some cases be premature, particularly where the breach occurs over a weekend/ or has significant impacts that are not known at the three-day mark.	IIROC recognizes that within three calendar days of discovery of the cybersecurity incident, a Dealer may have limited information regarding the cybersecurity incident. We expect Dealers to submit the best information available to the Dealer at the time of the reporting. In light of the nature of cybersecurity threats, it is in a Dealer's interest to be prepared to respond to such threats at any time, including over the weekend.
22.	The trigger for reporting should reflect PIPEDA's trigger from "the determination that a breach occurred" rather than "discovery of the breach".	We would expect that Dealers would interpret the trigger under Amendments and PIPEDA in materially the same manner.
23.	The 30-day follow-up report represents an additional burden not required by other regulatory bodies.	Together, the three-day and 30-day report required under the Amendments is intended to be consistent with the cybersecurity incident reporting required by other regulatory bodies, split between two reports submitted at two points in time following discovery of the cybersecurity incident. The three-day report reflects a brief snapshot of core information provided by a Dealer immediately following discovery of a cybersecurity incident. The 30-day report

	Summary of Comment	IIROC Response
		reflects a more detailed report produced after Dealers have had an opportunity to investigate a cybersecurity incident.
24.	The knowledge possessed by Dealers 30 days after a cybersecurity incident may be very limited, especially if there is an ongoing criminal investigation by a law enforcement agency. Dealers may not be in full possession of information required by the 30-day report. A premature analysis and assessment of a cybersecurity incident may prejudice Dealer by inviting unfair characterizations in later potential litigation. IIROC should consider only requiring a high level and factual description of the incident in the 30-day report, which would not be considered a "final" report, to the extent that such information is available to the Dealer.	We acknowledge that depending on the severity and complexity of a cybersecurity incident, a Dealer may conduct an investigation that extends beyond 30 days. In such instances, we expect Dealers to advise IIROC and discuss obtaining IIROC's agreement to extend the deadline for submitting the incident investigation report, as available under the Amendments. We expect factors such an ongoing criminal investigation or requiring further time to assess a cybersecurity incident as relevant factors in IIROC's determination to agree to an extension of the 30-day timeline.
25.	IIROC should consider changing the word "discovering" in DMR 3100(I)(B)(1.1)(2)/PLR 3703(vii)(a) and "discovered" in DMR 3100(I)(B)(1.1)(3)(ii)/ PLR 3703(vii)(a)(II) to the words "determining" and "determined", respectively. Most companies have a clear determination point in their incident response procedures that trigger a variety of next steps, whereas the "discovery" of an incident can be ambiguous. The determination point is usually based upon the completion of preliminary investigative steps that firms have identified as necessary to an effective cybersecurity incident response program. The proposed language would mitigate the risk of harm to Dealers resulting from premature and comprehensive reporting.	As noted above, we would interpret the words "discovery" and "determine" in the same manner.

	Summary of Comment	IIROC Response
Types of Incidents		
26.	IIROC should clarify how cybersecurity incidents originating from a source outside the firm (such as an identity theft with source at an unrelated retailer) that may impact a client's account are to be dealt with under this reporting regime. These incidents should not be subject to reporting requirements as they are not a cybersecurity breach.	The definition of "cybersecurity incident" under the Amendments may include those incidents that originate from a source outside a Dealer depending on the circumstances. The Dealer would have to consider the external source as part of the Dealer's information system. To determine if this type of cybersecurity incident triggers reporting under the Amendments, a Dealer ought to consider each part of the definition of "cybersecurity incident". A Dealer would be required to report the cybersecurity incident originating from a source outside the Dealer if the cybersecurity incident: • involved the unauthorized access, disruption or misuse of a Dealer's information system or information stored on such information system that • resulted in (or had a reasonable likelihood of resulting in) one of the enumerated grounds, including material impact on any part of the normal operations of the Dealer.
27.	If a Dealer has different divisions (e.g., Wealth Management and Securities Division), are they required to submit separate reports for the same incident involving the same clients?	The Amendments define cybersecurity incident in terms of the originating unauthorized act, rather than in terms of which clients were impacted. Accordingly, if the cybersecurity incident arose from the same act to gain unauthorized access to, disrupt or misuse the Dealer's

	Summary of Comment	IIROC Response
		information system, or information stored on such an information system, than we would expect a Dealer to submit one report.
28.	IIROC should consider adding a regulatory requirement that Dealers inform their Clearing Broker of a security breach. This is particularly significant in the case of Introducing Brokers where there may be an impact to the Risk Adjusted Capital as a result of the cybersecurity incident. If there is actual loss of capital resulting from the incident, there would be a material impact to the Clearing Broker with respect to the following functions: (a) Credit facilities extended to the Introducing Broker's customers to enable them to purchase securities on margin (b) Value added services such as Access to Desktop Technology and banking products (c) Financial and regulatory reporting.	We recognize the potential impact on Clearing Brokers as a result of an Introducing Broker experiencing a cybersecurity incident. However, the scope of the Amendments is restricted to reporting of cybersecurity incidents to IIROC, not the reporting obligations between Introducing and Clearing Brokers. We would encourage Introducing Brokers to ensure that there are sufficient contractual arrangements in place with their Clearing Broker to address reporting obligations between the parties as well as to appropriate regulatory authorities.
Sharing of Information		
29.	Information sharing, without expertise and established protocol, may expose the industry to further harm as result of notifying cybercriminals of areas of exposure or in respect of legal liability. Clients may be unnecessarily alarmed. Given the existence of information sharing organizations with the expertise to quickly detect, analyze and anonymize information, it is unclear whether IIROC's participation in this activity would be useful and may be detrimental.	The Amendments are consistent with IIROC's mission and the ongoing work that IIROC has conducted with Dealers since 2015. IIROC recognizes that organizations such as OSFI, whose jurisdiction does not reach all Dealers, has similarly recognized the growing importance of cybersecurity and accordingly has enhanced their monitoring of cyber threat and risk levels at Federally Regulated Financial Institutions.
30.	The process by which Dealers file cybersecurity incident reports should ensure that information, including the data involved, remains confidential and does not expose the firm	In recognition of the sensitive and confidential nature of information contained in a cybersecurity incident report,

	Summary of Comment	IIROC Response
	to further cyber incidents. IIROC should develop a secure, encrypted email or portal system to receive reports. Disclosing the names of reporting Dealers could be harmful to the trust and reputation of the firm. The names of reporting Dealers should be kept confidential from the public and other Dealers.	Dealers may submit a report to IIROC via secure means, such as in password protected or encrypted formats. Dealers have the flexibility to determine the best manner by which to submit their reports. We do not intend to disclose to the names of Dealers who have reported cybersecurity incidents to other Dealers or the public. We will anonymize any information about reported cybersecurity incidents that we share with the public or other Dealers.
31.	IIROC should clarify the scope, frequency, medium or timing of information shared about cybersecurity incidents with other parties. Will cybersecurity incidents reported to IIROC be shared with other Dealers, financial institutions, regulators and the general public? What level of information will be shared? Will the Dealer reporting the cybersecurity incident be identified? If not, how will the information be anonymized to limit the likelihood of identifying the reporting Dealer. The information sharing should be on an anonymous and high level to avoid causing undue harm to the reporting Dealer to undue panic among investors.	As noted in response to comment #30, respecting information shared publicly or with other Dealers, we will: • anonymize any information shared • not disclose the names of reporting Dealers • share cybersecurity incident information periodically, depending on the volume and nature of cybersecurity incidents that Dealers report to IIROC • share enough information about cybersecurity incidents reported to IIROC to sufficiently describe the nature of the incident and risk to other Dealers or investors while avoiding disclosing any information that could identify the affected Dealer. We expect to share cybersecurity incident information with regulatory bodies, such as the CSA, in a similar manner, although we may disclose the name of the affected Dealer when necessary.

	Summary of Comment	IIROC Response
32.	Will Dealers who want to receive threat intelligence information be required to sign a non-disclosure agreement prohibiting the recipient Dealers from disclosing threat information to third parties unless: (d) those parties are required to provide information security services to that Dealer and (e) those third parties have also signed the non-disclosure agreement.	We do not intend to require Dealers who want to receive threat intelligence information to sign a non-disclosure agreement. IIROC will anonymize any information relating to received cybersecurity incident reports before sharing with other Dealers.
Exemption		
33.	Many of the US state legislation on cybersecurity reporting include exceptions to account for investigations by law enforcement agencies. In these circumstances, prompt reporting may hinder the ongoing criminal investigation of the incident by the relevant law enforcement agency. Relevant law enforcement agencies may determine that investigations would be compromised by including detailed descriptions or assessments within the reports. IIROC should consider including a law enforcement exception that addresses both the reporting timeline and content of the reports.	We do not see an explicit exception as necessary. To the extent Dealers require an extension respecting the submission of the 30-day report, the Amendment expressly contemplate a Dealer seeking IIROC agreement to obtain such an extension.